UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,858	08/28/2002	Jurgen Lang	ACDPA-5003 PWO	1439

23416 7590 03/28/2006

CONNOLLY BOVE LODGE & HUTZ, LLP
P O BOX 2207
WILMINGTON, DE 19899

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/089,858	LANG ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 August 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/2/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-4 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-4 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1 and 4 uses the term "irreversible linking" The Examiner notes that the "irreversibility" of a cryptographic process has two major possible meanings in the art of cryptography, both of which apply with reasonable frequency. The first meaning is when a cryptographic process is applied in a such a manner that it would be infeasible to reverse the cryptographic process. For example, an encryption method using a large bit key may be "reversible" but may require a computer consuming the power of ten nuclear reactors to break within a span of 100 years. (Wikipedia "Bruce force attack") Such an encryption is occasionally referred to in the art as being "irreversible." In this instance, "irreversible" means "infeasible".

The second meaning of "irreversible" dictates a specialized cryptographic process such as a hash or one-way encryption. A hash is a cryptographic method by which data is processed into a

smaller representation of the data. For example, suppose that a data document consisted of 1000 bytes of information. As those skilled in the art recognize, a byte consists of 8 bits, and each bit consists of a 1 or 0 value. A byte therefore might store an example value as such 0110 1101 or 1111 1111 or 0000 0000.

A hash computation on the document might take the first bit of every single byte and put them together. In this case, the hash of the three bytes would yield "010"
Because the hash has been formed from taking into consideration only a small portion of the document, it is irreversible. That is, it is impossible to recomputed the values of the three bytes 0110 1101 or 1111 1111 or 0000 0000 from just the value "010"

Obviously the bytes hold far more information than can be extracted from the three bit hash. For this reason, a hash (also known as a one way encryption occasionally) is "irreversible"

The Applicant has not disclosed the nature of "irreversibility" used in claims 1 and 4. Given the context of its usage in the claims however, the Examiner shall interpret "irreversibly links" with the former interpretation.

Additionally, as further background information, suppose the value of one of the three bytes of the document was altered maliciously to become. 01101101 and 00001111 and 0000 0000

In this base, the hash would now read "000" and a detection could be made that the document is a forgery. While the Examiner's presented hash is not intended to be a full proof example of a hash, it is intended to provide background information as to how a hash may detect forgeries.

Additionally, Claim 1 further recites the limitations

- "whereby the security module generates a secret which remains unknown to a document producer"
- whereby it is not possible to draw conclusions about the secret.

The Examiner is uncertain how to interpret these limitations. Suppose the security module performs a hash on the document of the document producer. Does this satisfy the limitation of being unknown to the document producer?

Suppose the security module performs an encryption using a key that is known the document producer. Is this encryption "known" to the document producer? Clearly, the encryption while calculable by the document producer, the actual encrypted bits and bytes are not stored in the document producer's memory, but the memory of the security module.

For purposes of Examination, the Examiner will interpret "remains unknown to the document producer" as "a value that is not stored in the module local to the document producer"

With regards to the limitation "whereby it is not possible to draw conclusions about the secret", the Examiner notes that as long as the secret is a digital value, it is possible to perform some computation on it, or derive or "draw" a conclusion about the secret. For Example, suppose the secret consisted of the byte value 00001111. The NOT operation performed on this byte would yield 11110000. It can be concluded that the inverse of the secret is 11110000.

For this reason, the Examiner has interpreted this limitation to mean it is not possible to draw a conclusion, "where the conclusion is a determination of the value of the secret data" That is, "it is not possible to conclude the value of the secret"

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4 are rejected under 35 U.S.C. 102(b) as being anticipated by Houser et al, US patent 5606609.

In reference to claim 1:

Houser et al. discloses a method for producing forgery-proof documents or data records using a security module,

- Whereby the security module generates a secret which remains unknown to a document producer, where the secret is the embedded security object (Column 3, lines 50-60) & Figure 1, Item 130.
- Whereby the secret, together with information that reveals details about the identity of the security module, is transferred in encrypted form to an authentication unit, where the authentication unit is the electronic document security application (Column 3, lines 3, line 60 – Column 4, line 17) & (Column 12, lines 40-67)
- Whereby an authentication unit decrypts the secret, recognizes the identity of the security module and encrypts the secret, together with information on the identity of the document producer, in such a way that only a checking unit can carry out a decryption and then the authentication unit transmits these to the document producer, where the checking unit is the verification aspect of the security application (Column 4, lines 3-34)
- Whereby the document producer transfers its own data to the security module, (Figure 1, Items 110 to 130)
- Whereby the security module irreversibly links the secret with the data that the document producer itself has introduced, and (Column 3, lines 50-60) & (Column 13, lines 13-20) & (Column 15, lines 15-25)
- Whereby it is not possible to draw conclusions about the secret. (Column 4, lines 3-10)

Characterized in that the result of the irreversible linking of the secret with the data introduced by the document provider, the data introduced by the document producer itself as well as the

encrypted information of the authentication unit all serve to form the document that is transmitted to the checking unit. (Column 7, lines 65- Column 8, lines 20) (Figure 1, Items 140, 150) & (Column 3, lines 50-60)

In reference to claim 2:

Houser et al. (Column 10, line 60 – Column 11, line 10) & (Column 17, lines 30-60) discloses the method according to claim 1, characterized in that the additional information transferred by the authentication unit contains details on the identity of the document producer and on the period of validity of the documents generated by the document producer.

In reference to claim 3:

Houser et al. (Column 3, lines 50 – Column 4, lines 10) & (Column 4, lines 11 – 34) & (Column 21, lines 20-35) discloses the method for checking the authenticity of a document, characterized in that the checking unit checks whether the result of an irreversible linking of a secret with data introduced by a document producer have been incorporated into the document, in that the checking unit decrypts the secret and additional information that were encrypted by an authentication unit, in that the checking unit irreversibly links the decrypted secret with the data introduced into the document by the document producer, in the same manner as a security module used to produce the forgery-proof document, and in that the checking unit compares the result of the irreversible linking that it has performed itself with the result of an irreversible linking that was performed by the document producer and incorporated into the document, where the document is the document, where the irreversible linking of the secret is the embedding of

the security object into the document, where the checking unit is the verification unit, where the verification unit decrypts the embedded security object in order to validate the document.

In reference to claim 4:

Houser et al. (Column 4, lines 19-46) discloses the method according to claim 3, characterized in that the comparison determines whether data introduced into the document by the document producer has been forged.

Conclusion

6. The following art not relied upon is made of record:

- US patent 5937159, Meyers et al. discloses a method of controlling access of users to a database through authentication.
- US patent 5982506, Kara discloses a method of electronic document certification through encryption.

7. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

March 16th, 2006

Supervisory JACQUES H. LOUIS-JACQUES PRIMARY EXAMINER TC 2100